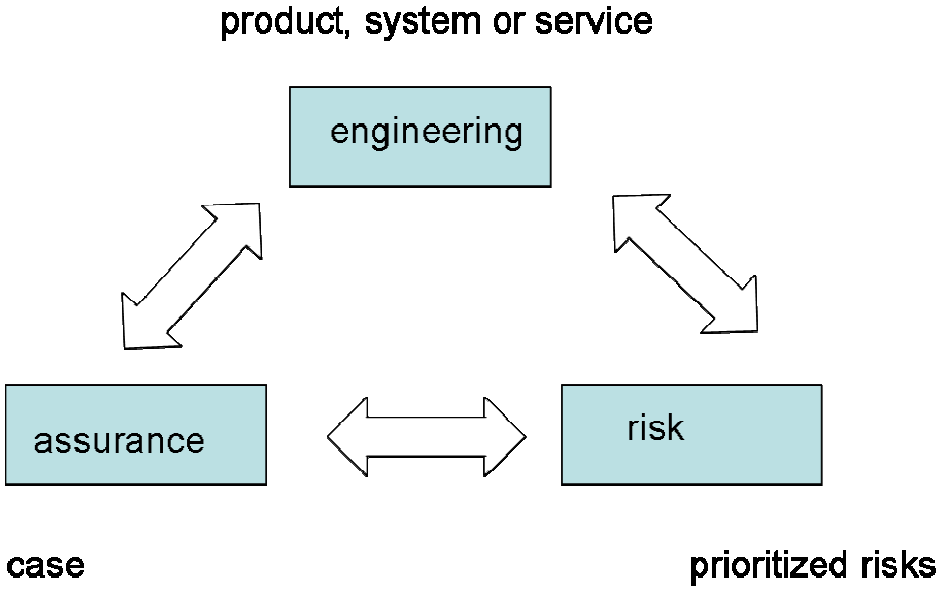
KDM Analytics™

Assurance Ecosystem

Djenana Campara
Chief Executive Officer, KDM Analytics
Board Director, Object Management Group (OMG)
Co-Chair Software Assurance and Architecture Driven Modernization TF, OMG

Engineering, Assurance and Risk

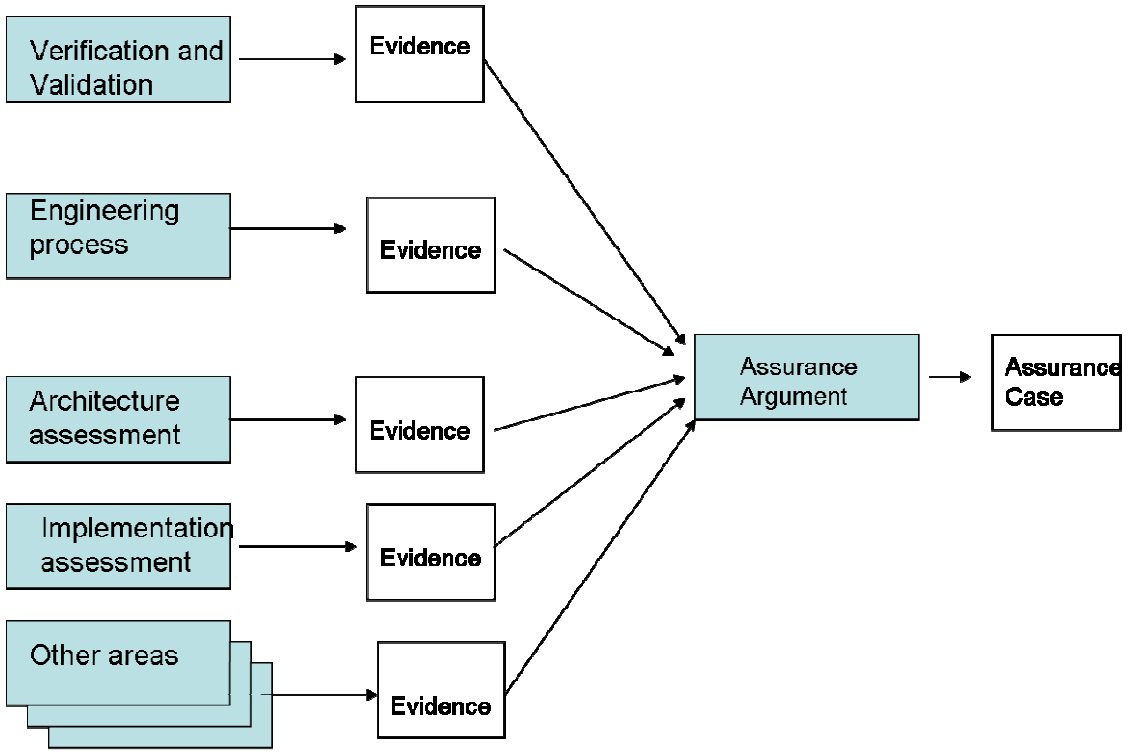
- Engineering, Assurance and Risk are intimately related
  - To assure a system means to ensure that System Engineering principles were correctly followed in meeting the security goals.
  - Additional guidance provided for System Assurance is based on the developing threats and prioritizing risks
- Today, the risk mgmt process often does not consider assurance issues in an integrated way
  - resulting in project stakeholders unknowingly accepting assurance risks that can have unintended and severe security issues.



System assurance can not and should not be executed as an isolated business process at a specific time in the program's schedule, but must be executed continuously from the very earliest conceptualization of the program, to its fielding and eventual disposal.

System Assurance - Reducing Uncertainty Associated with Vulnerability

- While Assurance does not provide additional security services or safeguards, it does serve to reduce the uncertainty associated with vulnerabilities resulting from
  - Bad practices
  - Incorrect safeguards
- Product of System Assurance is justified confidence delivered in the form of Assurance Case



TYPES OF EVIDENCES FOR ASSURANCE CASE

Confidence as a Product

- Confidence is produced by system assurance activities, which include a planned, systematic set of multi-disciplinary activities to achieve the acceptable measures of system assurance and manage the risk of exploitable vulnerabilities

- Characteristics of Confidence as a product
  - acceptable
  - reproducible
  - transferable
  - measurable

Producing and packaging confidence needs to be done in objective and cost-effective way

Achieving Comprehensiveness, Objectivity and Automation

Key Requirements

- Vulnerability knowledge is understood, captured and managed as assurance compliance points in the form of standardized specifications.
- Discovery and unified representation of system artifacts were higher level of abstractions (e.g. design, architecture and processes) do not loose its grounding traceability in the code
- Relation between discovered system artifacts and high level requirements, goals or policies that implemented artifacts represent, providing end-to-end traceability
- Standard based tooling environment that would provide higher automation in achieving the ultimate goal by integrating large set of tools to offset their limitations and weaknesses and integrating their strengths.

Software Assurance (SwA) Ecosystem – Standard-based Solution

- Standard-based integrated tooling environment that dramatically reduces the cost of multi-disciplinary software assurance activities

- Based on integrated ISO/OMG Open Standards
  - Semantics of Business Vocabulary and Rules (SBVR)
    - For formally capturing knowledge about vulnerabilities
  - Knowledge Discovery Metamodel (KDM)
    - Achieving system transparency in unified way
  - Software Assurance Metamodel: Argumentation Metamodel (ARM) and Software Assurance Evidence Metamodel (SAEM)
    - Intended for presenting Assurance Case and providing end-to-end traceability: requirement-to-artifact
  - Software Metrics Metamodel
    - Representing libraries of system and assurance metrics

SwA Ecosystem is expending: OMG SysA TF developing and integrating standards in area of Threat Risk Assessments and defining Security Vocabulary.

Compliance with Software Assurance (SwA) Ecosystem

- Pilot investment by DoD, NIST and DHS to demonstrate the value of SwA Ecosystem
  - 18 CWEs formalized (machine readable) into Software Fault Patterns – creating assurance compliance points
  - Test Case Generator to automatically produce test cases to evaluate/test static analysis tools
- DoD Research
  - Expending in area of Software Fault Patterns (SFP)
    - 50 SFP representing whitebox representation of 302 CWEs
- Open Source
  - GCC to KDM transparency – to be completed by April 2010
- Available SwA compliant tools
  - Assurance Case tool from Adelard and Artisan
  - KDM tools from KDM Analytics, Benchmark Consulting, MicroFocus, MIA-software (France)
  - SBVR tool from Business Semantics

Standard-based approach to Assurance ensures investment into coordinated strategy instead proprietary tools